BASF

We create chemistry

BASF Group -
Cyber Security Addendum

Version: 4.0

Date: 22.11.2023

Table of Contents

BASF
We create chemistry

1 Disclaimer

The Security Addendum contains requirements for information security.

All IT-suppliers are required to fulfill the specifications in the “General” chapter. The **other requirements** are **separated according to supplier type** and should be fulfilled accordingly. An explanation of the supplier types can be found at the beginning of the respective chapter.

For each supplier type, there are chapters describing specific risks and the goal to be achieved by addressing the risk. For this purpose, there are various measures of either a technical or organizational nature that can usually be applied. In case the risk is not relevant for a specific case or a supplier is of the opinion that a risk could be addressed in a different way than stated, there is the possibility to explain this briefly. It is up to BASF to decide if the given reasons and measures are sufficient.

2 Contact points for cyber security

In order to ensure seamless and efficient cooperation with our IT suppliers to maintain an appropriate level of cyber security, each supplier must designate contact persons and contact information for core cyber security roles.

The information is documented by the internal client (iBP or Purchasing) in Form *2 IT-Supplier Security Assessment_EN_Contact Sheet* in the current version in German or English for each supplier and sent to the Supplier Security team.

3 General

General Supplier Security is relevant if risks apply regardless of the service provided.

3.1 (Single) Point of Contact (SPoC) for Cyber Security / Information Security

Addressed risk Inadequate or delayed communication with suppliers on cyber security issues could result in vulnerabilities being addressed late or inadequately.

Goal Inquiries on cyber security issues, e.g. on implemented security measures or in case of discovery of security incidents affecting the supplier, will be answered within a reasonable period of time.

Technical Measures

G-T-01	Platform through which inquiries are submitted and answered promptly, e.g. ticket system

Organizational Measures

G-O-01	Point of contact for cyber security issues, e.g., CISO / Information Security Officer

3.2 Human Resources Security

Addressed risk The employees of suppliers could have a significant negative impact on the security level of BASF through their behavior, both intentionally and through carelessness.

Goal Only sufficiently qualified and aware employees are granted access to BASF information or systems.

Technical Measures

G-T-02	Role and authorization concept: Employees are given access only to information relevant to their work (need-to-know principle)

Organizational Measure

G-O-02	Regular awareness training on cyber security topics for all employees

3.3 Information Security Management

Addressed risk Insufficient conceptualization and operationalization of cyber security could result in vulnerabilities not being identified or avoided at an early stage. The exploitation of such vulnerabilities by an attacker could have a negative impact on the security level of BASF.

Goal Proactive design and management of the entirety of the supplier's security mechanisms.

Organizational Measures

G-O-03	Designation of a person responsible for maintaining an appropriate level of cyber security, e.g., CISO or Information Security Officer
G-O-04	Management of the entirety of all cyber security measures within the scope of an information security management system (ISMS)
G-O-05	Certification of the information security management system based on an established standard, e.g. ISO 27001

3.4 Supply Chain Security

Addressed risk Insufficient conceptualization and operationalization of cyber security could result in vulnerabilities not being identified or avoided at an early stage. The exploitation of such vulnerabilities by an attacker could have a negative impact on the security level of BASF.

Goal Require all material subcontractors and suppliers to establish and maintain an appropriate level of cyber security.

Organizational Measures	
G-O-06	Register of sub-suppliers engaged for the provision of services to BASF
G-O-07	Contractual obligation of subcontractors and suppliers to establish and maintain an appropriate level of cyber security

3.5 Change Management

Addressed risk Inadequate control of changes to provided services and products could result in information losses and performance degradation, which could have a negative impact on BASF's operations.

Goal Establish a standardized and formalized procedure for coordinating and committing to changes of provided services and products.

Technical Measures	
G-T-03	Platform through which all contract and service changes are managed and documented

Organizational Measures	
G-O-08	(Single) Point of Contact (SPoC) for changes in the contracted services

3.6 Compliance

Addressed risk BASF could be held liable for violations of laws and regulations caused by suppliers.

Goal All applicable compliance requirements are adhered to at all times.

Organizational Measures

G-O-09	Designation of a person responsible for maintaining global compliance, e.g. compliance officer
G-O-10	Management of all compliance measures within the scope of a compliance management system (CMS)

4 Consulting Services

All consulting services that are directly or indirectly related to organizational development, as well as the provision, operation or decommissioning of IT solutions.

4.1 Resource Management

Addressed risk Staff shortages could result in contractually agreed services not being provided.

Goal It is guaranteed at all times that sufficiently qualified employees are available for the delivery of the contractually agreed services. All services can be delivered on time and in the agreed quality.

Organizational Measures

C-O-01	Management of human resources within the scope of internal resource management to provide qualified personnel
C-O-02	Training and development concept for specialist and managerial staff

4.2 Information Handling

Addressed risk Information used within consulting projects could compromise BASF's cyber security if confidentiality is lost.

Goal It is ensured at all times that all information created and received within the scope of consulting projects is treated confidentially and protected from being compromised.

Technical Measures

C-T-01	Encryption of e-mail communication using an established industry standard, e.g. PGP, S/MIME
C-T-02	Encryption of hard drives of mobile devices, e.g. BitLocker, Vera Crypt

C-T-03	Encryption of server hard drives, e.g. BitLocker, Vera Crypt
C-T-04	Encryption of mobile data carriers, e.g. BitLocker, Vera Crypt, hardware encryption
C-T-05	Management of all permissions within the scope of end-to-end identity and access management (IAM)
Organizational Measures	
C-O-03	Policy for storing, processing and sending information before, during and after projects
C-O-04	Security incident handling process
C-O-05	Process for remote data wiping in the event of loss of mobile devices
C-O-06	Process to ensure that only employees who provide consulting services for BASF have access to BASF information (need-to-know principle)
C-O-07	Process for granting, changing or revoking access rights when employees join or leave the company or change roles (Joiner-Mover-Leaver process)
C-O-08	Classification concept for processed information based on its criticality

4.3 Malware Protection

Addressed risk If IT devices used in the consulting process are compromised, information could be unintentionally changed or made accessible to unauthorized third parties.

Goal It is ensured that no malware can be installed on the IT devices.

Technical Measures	
C-T-06	Malware protection solution for servers
C-T-07	Malware protection solution on clients, e.g. Microsoft Defender
C-T-08	Security appliances, e. g. Firewall, SIEM
C-T-09	Suitable segmentation of the corporate network based on criticality regarding confidentiality and availability requirements of processed data
C-T-10	Use of a sandbox solution to open unknown files or files from unknown senders.
C-T-11	Centrally managed software distribution
C-T-12	No granting of local administration rights to users

Organizational Measures	
C-O-09	Process for immediate installation of security-relevant updates of all software solutions in use
C-O-10	Hardening policy for servers

C-O-11	Hardening policy for clients
C-O-12	Hardening policy for smartphones

4.4 Data Backup

Addressed risk System errors, malware or misuse of IT systems could result in the loss of data collected within the scope of a consulting project.

Goal All data relevant to BASF is backed up regularly and can be restored in the event of data loss.

Technical Measures

C-T-13	Regular, automated backup of all data relevant to BASF

Organizational Measures

C-O-13	Data backup concept
C-O-14	Regular exercises in data backup and recovery

4.5 Physical Security

Addressed risk When being processed in supplier's premises, BASF information could be compromised by external parties.

Goal All information from and about BASF is protected from physical access by unauthorized third parties.

Technical Measures	
C-T-14	Lockable offices
C-T-15	Lockable cabinets or safes
Organizational Measures	
C-O-15	Policy on accompanying guests in the supplier's properties by employees
C-O-16	Policy for locking data storage media, IT equipment and documents

4.6 Protection of Personal Identifiable Information (PII)

Addressed risk When processing PII within the scope of contracted processing, personal rights of data subjects could be compromised by improper use of information.

Goal When processing PII, it is ensured at all times that the requirements of the GDPR and downstream data protection regulations are complied with.

Organizational Measures

C-O-17	Designation of a person responsible for data protection, e.g. data protection officer
C-O-18	Protection of the totality of all personal identifiable information within the scope of a data protection management system (DMS)

5 Service & Support

All service and support services within the scope of which solutions are administered, maintained or disposed of. This covers the entire product life cycle of a solution and begins with installation and ends with disposal.

5.1 Resource Management

Addressed risk Staff shortages could result in contractually agreed services not being provided.

Goal It is guaranteed at all times that sufficiently qualified employees are available for the delivery of the contractually agreed services. All services can be delivered on time and in the agreed quality.

Organizational Measures

S-O-01	Management of human resources within the scope of internal resource management to provide qualified personnel
S-O-02	Training and development concept for specialist and managerial staff

5.2 Information Handling

Addressed risk Information used within services and support assignments could compromise BASF's cyber security if confidentiality is lost.

Goal It is ensured at all times that all information created and received within the scope of services and support activities is treated confidentially and protected from being compromised.

Technical Measures

S-T-01	Encryption of e-mail communication using an established industry standard, e.g. PGP, S/MIME
S-T-02	Encryption of hard drives of mobile devices, e.g. BitLocker, Vera Crypt

S-T-03	Encryption of server hard drives, e.g. BitLocker, Vera Crypt
S-T-04	Encryption of mobile data carriers, e.g. BitLocker, Vera Crypt, hardware encryption
S-T-05	Management of all permissions within the scope of end-to-end identity and access management (IAM)
Organizational Measures	
S-O-03	Policy for storing, processing and sending information before, during and after assignments
S-O-04	No granting of local administration rights to users
S-O-05	Process for remote data wiping in the event of loss of mobile devices
S-O-06	Process to ensure that only employees who provide consulting services for BASF have access to BASF information (need-to-know principle)
S-O-07	Process for granting, changing or revoking access rights when employees join or leave the company or change roles (Joiner-Mover-Leaver process)
S-O-08	Classification concept for processed information based on its criticality

5.3 Malware Protection

Addressed risk If IT devices used in services and support assignments are compromised, information could be unintentionally changed or made accessible to unauthorized third parties.

Goal It is ensured that no malware can be installed on the IT devices.

Technical Measures

S-T-06	Malware protection solution for servers
S-T-07	Malware protection solution on clients, e.g. Microsoft Defender
S-T-08	Security appliances, e. g. Firewall, SIEM
S-T-09	Suitable segmentation of the corporate network based on criticality regarding confidentiality and availability requirements of processed data
S-T-10	Use of a sandbox solution to open unknown files or files from unknown senders.
S-T-11	Centrally managed software distribution
S-T-12	No granting of local administration rights to users

Organizational Measures

S-O-09	Process for immediate installation of security-relevant updates of all software solutions in use
S-O-10	Hardening policy for servers

S-O-11	Hardening policy for clients
S-O-12	Hardening policy for smartphones

5.4 Data backup

Addressed risk System errors, malware or misuse of IT systems could result in the loss of data which is relevant to BASF.

Goal All data relevant to BASF is backed up regularly and can be restored in the event of data loss.

Technical Measures

S-T-13	Regular, automated backup of all data relevant to BASF

Organizational Measures

S-O-13	Data backup concept
S-O-14	Regular exercises in data backup and recovery

5.5 Physical Security

Addressed risk When being processed in supplier's premises, BASF information could be compromised by external parties.

Goal All information from and about BASF is protected from physical access by unauthorized third parties.

Technical Measures	
S-T-14	Lockable offices
S-T-15	Lockable cabinets or safes
Organizational Measures	
S-O-15	Policy on accompanying guests in the supplier's properties by employees
S-O-16	Policy for locking data storage media, IT equipment and documents

5.6 Protection of Personal Identifiable Information (PII)

Addressed risk When processing PII within the scope of contracted processing, personal rights of data subjects could be compromised by improper use of information.

Goal When processing PII, it is ensured at all times that the requirements of the GDPR and downstream data protection regulations are complied with.

Organizational Measures

S-O-17	Designation of a person responsible for data protection, e.g. data protection officer
S-O-18	Protection of the totality of all personal identifiable information within the scope of a data protection management system (DMS)

5.7 Remote Access

Addressed risk Remote access sessions could be used by unathorized persons as a gateway into the BASF network. Insecure protocols, configurations, passwords and applications could allow unauthorized access.

Goal During any remote access, the protection of stored, processed and transmitted information and data as well as the integrity of the BASF infrastructure is ensured.

Technical Measures

S-T-16	Use of secure protocols, encryption methods and applications when accessing BASF data and infrastructure

Organizational Measures

S-O-19	Full documentation or recording of all remote access sessions

5.8 IT Administration

Addressed risk Improper IT administration could lead to a disruption or compromise of BASF's infrastructure.

Goal All service and support activities are performed in compliance with industry best practices for secure administration.

Technical Measures	
S-T-17	Ticket system for the management of service and support requests
Organizational Measures	
S-O-20	Management and documentation of tools used by service and support staff
S-O-21	Immediate installation of security-relevant updates and patches of all software solutions used
S-O-22	Process for performing the service and support activities being provided.

6 Hardware Components

Procurement of individual hardware components that are installed in endpoints or for whose use an endpoint is required, e.g. mouse, keyboard, screen, RAM, hard disks, etc.

6.1 Delivery

Addressed risk Hardware components could be damaged during the delivery process. In addition, components could be manipulated to compromise the BASF infrastructure.

Goal All hardware components are delivered fully functional and in the intended configuration in an integer condition.

Technical Measures	
H-T-01	Platform for receiving, processing and resolving complaints and returns
H-O-01	Process to ensure the completeness of each delivery before shipment
Organizational Measures	
S-O-02	Real time shipment tracking
S-O-03	Protection of shipments from damage
S-O-04	Sealing of all shipments

6.2 Product Security

Addressed risk Unsuitable, damaged or manipulated components could lead to disruptions or compromise of the BASF infrastructure.

Goal All hardware components are tested in terms of functionality and integrity by the supplier or an upstream supplier. Sufficient technical documentation is available for all hardware components to select the optimal components for a given application.

Organizational Measures

H-O-05	Documentation of the ideal operating environment for all components
H-O-06	Process for validating the functionality and integrity of all components by the supplier or an upstream supplier

7 Endpoint & Appliances

Procurement of devices planned for use by end users or in the data center, e.g., laptops, smartphones, servers, etc., as well as appliances (single-purpose devices / devices with specialized operating systems that are essential for operation), such as firewalls, VPN gateways, routers or switches.

7.1 Delivery

Addressed risk Devices could be damaged during the delivery process. In addition, components could be manipulated to compromise the BASF infrastructure.

Goal All evidence are delivered fully functional and in the intended configuration in an integer condition.

Technical Measures	
E-T-01	Platform for receiving, processing and resolving complaints and returns

Organizational Measures	
E-O-01	Process to ensure the completeness of each delivery before shipment
E-O-02	Real time shipment tracking
E-O-03	Protection of shipments from damage
E-O-04	Sealing of all shipments

7.2 Product Security

Addressed risk Unsuitable, damaged or manipulated devices could lead to disruptions or compromise of the BASF infrastructure.

Goal All devices are tested in terms of functionality and integrity by the supplier or an upstream supplier. Sufficient technical documentation is available for all hardware components to select the optimal components for a given application.

Organizational Measures

E-O-05	Documentation of the ideal operating environment for all components
E-O-06	Process for validating the functionality and integrity of all components by the supplier or an upstream supplier

7.3 Device Setup

Addressed risk When devices are initially set up by the vendor, using common and thus easily guessable default configurations could enable attackers to compromise BASF.

Goal Security-related updates and patches available at the time of installation are installed on all devices. Initial passwords are configured so that they must be changed by the user at the first login.

Organizational Measures

E-O-07	Installation of all available updates and patches for the operating system and firmware
E-O-08	Use of initial passwords, which must be changed when the device is used for the first time
E-O-09	Avoiding the installation of software packages that are not essential, e.g. optional OEM software

8 On-Premise Solutions

Procurement of application (packages) that are run on BASF infrastructure (e.g. on laptops, servers or smartphones) and do not require access to the manufacturer's systems for use.

8.1 IT Security Concept

Addressed risk If industry-standard security mechanisms are not taken into account during planning and development, or if the interactions between measures are not recognized, attackers could exploit the resulting security vulnerabilities and compromise BASF's information, data and infrastructure.

Goal The entirety of all security measures for a solution are defined within the scope of an IT security concept, and the implementation status is continuously documented and updated when changes are made.

Organizational Measures	
O-O-01	Development of an IT security concept for the solution
O-O-02	Update of the IT security concept on a regular basis and in case of changes
O-O-03	Provision of documentation of implemented security mechanisms to BASF

8.2 Cryptography

Addressed risk If data is not protected during storage, processing or transmission, it could be intercepted or compromised by unauthorized third parties.

Goal During the entire lifecycle, data is protected from unauthorized access.

Technical Measures	
O-T-01	Encryption of data during transfer (Data at Transit), e.g. HTTPS, SSH

O-T-02	Encryption of data during storage, e.g. database encryption
O-T-03	Multi-factor authentication for access to sensitive information
O-T-04	Multi-factor authentication for configuration changes
Organizational Measures	
O-O-04	Crypto concept with all implemented encryption methods and key lengths

8.3 Roles and Permissions Concept

Addressed risk A missing or inadequate roles and permissions concept could enable unauthorized users to gain access to sensitive information.

Goal Roles and permissions can be managed granularly so that users only have access to the information they need to perform their tasks.

Technical Measures	
O-T-05	Active Directory API
O-T-06	LDAP API
O-T-07	Assignment of permissions exclusively via the assignment of roles
O-T-08	Software module / component / function for roles and permissions management

Organizational Measures

O-O-05	Formalized and documented roles and permissions concept

8.4 Updates and Patches

Addressed risk If security-relevant updates and patches are not installed immediately after their release, attackers could reconstruct the vulnerability addressed by the update or patch and actively exploit it.

Goal The time between the release of updates and patches, their provision to BASF, and their installation is so short that it makes it impossible for attackers to actively exploit known vulnerabilities that have not been fixed.

Technical Measures

O-T-09	Provision of security-related updates and patches within the solution
O-T-10	Provision of security-related updates and patches via the supplier's website

Organizational Measures

O-O-06	Information about newly released updates and patches via e-mail
O-O-07	Information about newly released updates and patches within the solution
O-O-08	Information about newly released updates and patches via the supplier's website

8.5 Penetration Testing

Addressed risk The complexity of solutions can result in vulnerabilities remaining unnoticed due to the interaction of subcomponents and resulting effects. Such blind spots could be exploited by attackers.

Goal The level of protection of the overall solution is regularly reviewed, taking into account all known attack methods, and further developed based on the findings.

Organizational Measures

O-O-09	Regular penetration testing of the solution
O-O-10	Event-driven penetration tests of the solution, e.g. in case of significant changes
O-O-11	Regular penetration tests of third-party components, e.g. software modules from external developers
O-O-12	Event-driven penetration tests of third-party components, e.g., when security vulnerabilities or security incidents are identified

8.6 Support and Documentation for Users

Addressed risk Missing or unavailable user instructions could result in users not using the solution or using it incorrectly. This could have an adverse effect on BASF's operations.

Goal All user(s) groups are enabled to use the solution in the intended manner for the intended purpose.

Technical Measures

O-T-11	Community forum for exchange between users

O-T-12	Helpdesk website for users
O-T-13	Phone hotline for users
O-T-14	Support via e-mail for users
Organizational Measures	
O-O-13	Training offered for user (groups) by the supplier's own trainers
O-O-14	Training offered to user (groups) by external training providers, e.g., industry associations, TÜV (German Technical Inspection Association)
O-O-15	Self-study materials for user (groups), e.g. tutorial videos, presentations, step-by-step instructions
O-O-16	General user manuals
O-O-17	Scenario-based user manuals

8.7 Support and Documentation for Administrators

Addressed risk Improper installation, distribution or configuration could result in compromised data or failure of the solution, thereby disrupting BASF's operations.

Goal BASF administrators responsible for operating the solution are enabled to manage the solution as intended.

Technical Measures

O-T-15	Community forum for exchange between administrators
O-T-16	Helpdesk website for administrators
O-T-17	Phone hotline for administrators
O-T-18	Support via e-mail for administrators

Organizational Measures

O-O-18	Training offered for administrators by the supplier's own trainers
O-O-19	Training for administrators offered by external training providers, e.g., industry associations, TÜV (Technical Inspection Agency)
O-O-20	Self-study materials for administrators, e.g. tutorial videos, presentations, step-by-step instructions
O-O-21	General administrator manuals
O-O-22	Scenario-based administrator manuals

8.8 Software Architecture

Addressed risk If access from outside the BASF infrastructure via the Internet is allowed, attackers could exploit functional and architectural vulnerabilities to retrieve data or, in the case of successful attacks, gain access to other systems within the BASF infrastructure via privilege escalation.

Goal Both the architecture and the processes for data processing are designed to protect the solution and the processed data from unauthorized access and to ensure that no other BASF systems are affected if individual components are compromised.

Technical Measures

O-T-19	3-tier architecture: separation of the presentation, processing and data storage layers
O-T-20	2-tier architecture: separation of the application and data storage layers
O-T-21	Protection against cross-site scripting
O-T-22	Input validation to protect against unauthorized data manipulation, e.g. via SQL injection

Organizational Measures

O-O-23	Documentation of the solution's architecture

9 Cloud Solutions

Procurement of application (packages) that are operated on the infrastructure of a service provider and whose use requires mandatory internet access. It is irrelevant whether a solution is SaaS (Software-as-a-Service), PaaS (Platform-as-a-Service), Iaas (Infrastructure-as-a-Service) or a cloud technology that is not specific here.

9.1 IT Security Concept

Addressed risk If industry-standard security mechanisms are not considered during planning and development, or if the interactions between measures are not identified, attackers could exploit the resulting vulnerabilities and compromise BASF's information, data and infrastructure.

Goal The entirety of all security measures for a solution are defined within the scope of an IT security concept, and the implementation status is continuously documented and updated when changes are made.

Organizational Measures	
CL-O-01	Development of an IT security concept for the solution
CL-O-02	Update of the IT security concept on a regular basis and in case of changes
CL-O-03	Provision of documentation of implemented security mechanisms to BASF

9.2 Cryptography

Addressed risk If data is not protected during storage, processing or transmission, it could be intercepted or compromised by unauthorized third parties.

Goal During the entire lifecycle, data is protected from unauthorized access.

Technical Measures	
CL-T-01	Encryption of data during transfer (Data at Transit), e.g. HTTPS, SSH

CL-T-02	Encryption of data during storage, e.g. database encryption
CL-T-03	Multi-factor authentication for access to sensitive information
CL-T-04	Multi-factor authentication for configuration changes
Organizational Measures	
CL-O-04	Crypto concept with all implemented encryption methods and key lengths

9.3 Roles and Permission Concept

Addressed risk A missing or inadequate roles and permissions concept could enable unauthorized users to gain access to sensitive information.

Goal Roles and permissions can be managed granularly so that users only have access to the information they need to perform their tasks.

Technical Measures

CL-T-05	Active Directory API
CL-T-06	LDAP API
CL-T-07	Assignment of permissions exclusively via the assignment of roles
CL-T-08	Software module / component / function for roles and permissions management

Organizational Measures

CL-O-05	Formalized and documented roles and permissions concept

9.4 Malware Protection

Addressed risk If systems are compromised, information could be unintentionally changed or made accessible to unauthorized third parties.

Goal It is ensured that no malware can be installed on IT devices.

Technical Measures

CL-T-09	Malware protection solution for servers
CL-T-10	Malware protection solution on clients, e.g. Microsoft Defender
CL-T-11	Security appliances, e. g. Firewall, SIEM
CL-T-12	Suitable segmentation of the corporate network based on criticality regarding confidentiality and availability requirements of processed data
CL-T-13	Use of a sandbox solution to open unknown files or files from unknown senders.
CL-T-14	Centrally managed software distribution
CL-T-15	No granting of local administration rights to users

Organizational Measures	
CL-O-06	Process for immediate installation of security-relevant updates of all software solutions in use
CL-O-07	Hardening policy for servers
CL-O-08	Hardening policy for clients
CL-O-09	Hardening policy for smartphones

9.5 Data Backup

Addressed risk System errors, malware or misuse of IT systems could result in the loss of data.

Goal All data relevant to BASF is backed up regularly and can be restored in the event of data loss.

Technical Measures	
CL-T-16	Regular, automated backup of all data relevant to BASF
CL-T-17	Automated deployment workflow e.g. CI/CD

Organizational Measures	
CL-O-10	Data backup concept

CL-O-11	Regular exercises in data backup and recovery
CL-O-12	Manual snapshots of system states prior to any changes to the systems and application(s) required to run the solution

9.6 Penetration Testing

Addressed risk The complexity of solutions can result in vulnerabilities remaining unnoticed due to the interaction of subcomponents and resulting effects. Such blind spots could be exploited by attackers.

Goal The level of protection of the overall solution is regularly reviewed, taking into account all known attack methods, and further developed based on the findings.

Organizational Measures

CL-O-13	Regular penetration testing of the solution
CL-O-14	Event-driven penetration tests of the solution, e.g. in case of significant changes
CL-O-15	Regular penetration tests of third-party components, e.g. software modules from external developers
CL-O-16	Event-driven penetration tests of third-party components, e.g., when security vulnerabilities or security incidents are identified

9.7 Support and Documentation for Users

Addressed risk Missing or unavailable user instructions could result in users not using the solution or using it incorrectly. This could have an adverse effect on BASF's operations.

Goal All user(s) groups are enabled to use the solution in the intended manner for the intended purpose.

Technical Measures	
CL-T-18	Community forum for exchange between users
CL-T-19	Helpdesk website for users
CL-T-20	Phone hotline for users
CL-T-21	Support via e-mail for users
Organizational Measures	
CL-O-17	Training offered for user (groups) by the supplier's own trainers
CL-O-18	Training offered to user (groups) by external training providers, e.g., industry associations, TÜV (German Technical Inspection Association)
CL-O-19	Self-study materials for user (groups), e.g. tutorial videos, presentations, step-by-step instructions
CL-O-20	General user manuals
CL-O-21	Scenario-based user manuals

9.8 Support and Documentation for Administrators

Addressed risk Improper installation, distribution or configuration could result in compromised data or failure of the solution, thereby disrupting BASF's operations.

Goal BASF administrators responsible for operating the solution are enabled to manage the solution as intended.

Technical Measures

CL-T-22	Community forum for exchange between administrators
CL-T-23	Helpdesk website for administrators
CL-T-24	Phone hotline for administrators
CL-T-25	Support via e-mail for administrators

Organizational Measures

CL-O-22	Training offered for administrators by the supplier's own trainers
CL-O-23	Training for administrators offered by external training providers, e.g., industry associations, TÜV (Technical Inspection Agency)
CL-O-24	Self-study materials for administrators, e.g. tutorial videos, presentations, step-by-step instructions
CL-O-25	General administrator manuals

CL-O-26	Scenario-based administrator manuals

9.9 Software Architecture

Addressed risk Attackers could exploit vulnerabilities in the software architecture to retrieve data or, in the case of successful attacks, gain access to other systems within the BASF infrastructure via privilege escalation.

Goal The software architecture is designed to protect the solution and the processed data from unauthorized access and to ensure that no other BASF systems are affected if individual components are compromised.

Technical Measures

CL-T-26	3-tier architecture: separation of the presentation, processing and data storage layers
CL-T-27	2-tier architecture: separation of the application and data storage layers
CL-T-28	Protection against cross-site scripting
CL-T-29	Input validation to protect against unauthorized data manipulation, e.g. via SQL injection

Organizational Measures

CL-O-27	Documentation of the solution's architecture

9.10 Business Continuity Management

Addressed risk The failure or malfunction of critical system components can lead to losses in availability of cloud solutions. Particularly in the case of critical business processes, even a short outage can lead to considerable damage for BASF.

Goal Meeting the agreed service level agreements (SLAs) can be ensured for the entire duration of the contract.

Technical Measures	
CL-T-30	Emergency data center

Organizational Measures	
CL-O-28	Designation of a responsible person for emergency management, e.g. BCM officer, emergency officer
CL-O-29	Management of the entirety of all emergency management measures within the scope of a Business Continuity Management System (BCMS)
CL-O-30	Redundancy concept

9.11 Protection of Personal Information (PII)

Addressed risk When processing PII within the scope of contracted processing, personal rights of data subjects could be compromised by improper use of information.

Goal When processing PII, it is ensured at all times that the requirements of the GDPR and downstream data protection regulations are complied with.

Organizational Measures	
CL-O-31	Designation of a person responsible for data protection, e.g. data protection officer

CL-O-32	Protection of the totality of all personal identifiable information within the scope of a data protection management system (DMS)

9.12 Physical Security

Addressed risk If cloud solutions are operated in unsecured data centers, servers and other IT components can be manipulated, stolen or destroyed.

Goal All infrastructure required to provide the cloud solution is operated in a secure data center.

Technical Measures

CL-T-31	Fire extinguishing and prevention system
CL-T-32	Multiple fire compartments
CL-T-33	Hazard alarm system
CL-T-34	Video surveillance system
CL-T-35	Automated monitoring of the infrastructure
CL-T-36	Connection of the data center to a central, 24/7 manned control station
CL-T-37	Temperature and humidity management
CL-T-38	Uninterruptible power supply

CL-T-39	Surge protection device
Organizational Measures	
CL-O-33	Dust protection measures
CL-O-34	Access control concept

10 Software Development

Development of software solutions or components that are used stand-alone or in integration with other solutions. This also includes customization of solutions. The configuration of a solution does not fall under Software Development.

Note on application: The requirements for software development are to be fulfilled in addition to the service types On-Premise Solutions and Cloud Solutions when suppliers develop solutions themselves.

10.1 Development Process

Addressed risk If best practices for secure software development are not applied, this can lead to security vulnerabilities which could be exploited by attackers. This applies to both the source code and the configuration of provided installation media.

Goal A standardized and managed development process ensures that all known vulnerabilities in the software (packages) in use are closed and that installation media are configured in a sufficiently secure manner before deployment.

Technical Measures	
SW-T-01	Automated deployment workflow, e.g. CI/CD

Organizational Measures	
SW-O-01	Formalized Secure Software Development Life Cicle (SSDLC)
SW-O-02	Management and documentation of the tools used in the development process
SW-O-03	Testing new versions of the solution based on standardized test cases
SW-O-04	Conducting unit tests

SW-O-05	Conducting load tests
SW-O-06	Adherence to the principle: Security by Design
SW-O-07	Adherence to the principle: Security by Default
SW-O-08	Adherence to the principle: Privacy by Design
SW-O-09	Adherence to the principle: Privacy by Default

10.2 Third-Party Software

Addressed risk When using third-party software components, such as software modules from external developers, vulnerabilities in these components could serve as attack vectors for attackers to gain unauthorized access to data.

Goal All third-party software components are regularly checked for vulnerabilities. Security-relevant updates and patches of external components are provided by the supplier via the general updates and patches channel agreed for the solution.

Organizational Measures

SW-O-10	Register of all third-party software components
SW-O-11	Periodic testing process for known vulnerabilities of the third-party software components in use.